



**Patchogue-Medford Union Free School District**

---

**Review of Information Technology Inventory and  
Protection of Personal, Private and Sensitive Information  
(PPSI) on Mobile Computing Devices**

**For the 2020-2021 School Year**

September 2021

The Board of Education  
Patchogue-Medford Union Free School District  
241 South Ocean Avenue  
Patchogue, NY 11772

Board of Education:

We have been retained to function as the internal auditor for the Patchogue-Medford Union Free School District (hereinafter, “the District”). Our responsibility is to assess internal control systems in place within the District, and to make recommendations to improve upon possible control weaknesses or deficiencies. In doing so, we hope to provide assurance to the District’s Board, management, and residents that the fiscal operations of the District are being handled appropriately and effectively.

### **BACKGROUND**

We assessed certain aspects of the District information technology (IT) environment and issued a report of our review in December 2017. Technology has shifted from the traditional desktop environment to handheld devices that permit users to perform similar functions without being constricted to one location. Such mobile computing devices (MCDs) include tablets, smartphones, personal digital assistants (PDAs), laptops, and netbooks. While such portability has facilitated employee productivity, expanded learning opportunities for students, and allowed for greater and faster communications, these devices can introduce security vulnerabilities.

### **PURPOSE**

Due to COVID-19, school districts across the State had to cease in-person instruction in mid-March 2020. At that time, the District started distributing the available laptops to students and staff to enable them to operate remotely. The District’s opening plan for the 2020-2021 school year necessitated continued remote learning; therefore, all students and staff needed appropriate devices to connect to the District. This included purchasing laptops, additional desktops for the classrooms, webcams, and internet access devices. The District utilizes an online application system, FreshWorks, to track such inventory. The purpose of our review was to determine whether the internal controls are sufficient to ensure that IT equipment purchased as a result of the pandemic is properly safeguarded and inventoried.

### **SCOPE**

The scope of this review entailed gaining an understanding of the internal controls to protect such devices and the information contained within them. This was accomplished by:

- Reviewing the current policies and procedures in place related to IT inventory as well as policies that address the risks of exposure of PPSI and effectively protecting computing devices;
- Assessing the procedures for tracking and safeguarding computer equipment, including when equipment is transferred or deemed obsolete; and

- Testing a sample of IT equipment to determine the completeness and accuracy of the District's inventory information maintained in FreshWorks.

### CONCLUSION:

The District is utilizing an IT inventory tracking system and is working to ensure the inventory records are accurate. While we noted controls have been implemented, we noted areas where controls could be improved. Sections I and II describe the results of our review and provide recommendations to improve the internal controls surrounding computer equipment inventory and access controls in the District.

---

### I. POLICIES & PROCEDURES

Good governance and accountability require the District's Board to adopt policies and procedures related to IT to provide criteria and guidance for the District's computer-related operations. To effectively protect computing resources and data, districts should have an acceptable use policy to inform users about appropriate and safe use of District computers, a hardware sanitization policy to ensure that equipment is not discarded with sensitive data and a breach notification policy in the event that sensitive data is compromised. These policies should be reviewed periodically and updated, as necessary, to reflect changes in technology or a district's computing environment. A district's Board is responsible for this review and update process.

Since devices have become more mobile, district officials are responsible for implementing policies and procedures that ensure the security of district MCDs. The NYS OSC has issued guidance that policies should also define which devices are covered (e.g., district-owned or personally-owned), and should indicate the "procedures for reporting lost or stolen MCDs and storage devices, the process used for gaining approval before connecting new devices to the system, and user responsibilities." Districts should have specific care and use guidelines for all district-owned MCDs that are given to staff/students and should require staff/students to sign an agreement regarding care and use of district-owned MCDs.

The District has adopted several IT policies which include:

- **Policy 3461 Capital Assets Accounting Procedures**, which defines the proper control and preservation of District capital assets and the maintenance of inventory records.
- **Policy 3801 Secure Data Destruction Policy**, which defines guidelines for the disposal of technology equipment and components owned by the District to protect sensitive data.
- **Policy 3802 Technology Security for Personal Private and Sensitive Information**, which further addresses the security of PPSI.
- **Policy 3803 Computer Password Policy**, which outlines employee password requirements and guidelines.
- **Policy 4410 Technology Acceptable Use Policy for Employees and Volunteers and Policy 4410-R Technology Acceptable use**, which addresses the expectations of personal safety, system security, legal activities, inappropriate access to materials for all individuals who utilize the District's technology.
- **Policy 4411 Remote Access to Computer Network**, which addresses standards for connecting to the District's network from any external host to minimize the potential exposure from damages from unauthorized use of the Districts resources.

- **Policy 4412 Information Security Breach and Notification and Policy 4412-R Information Security Breach and Notification Regulation**, which detail how the District would notify an individual(s) whose private information was or is reasonably believed to have been compromised.
- **Policy 4420 Computer Controls Policy for Financial Software**, which addresses “the importance of ensuring that the District’s financial accounting software (nVision) and the financial network facilities are adequately secured.
- **Policy 5119 Security of Information -- District-Leased Computer System**, which restricts the access and use of District computers and sensitive data.

In addition, the District has implemented a process whereby students and teachers using a District laptop complete and sign an agreement outlining the responsibilities of the individual/family with regard to the device. A similar agreement is completed for any individual using a District hotspot device.

Managing and tracking inventory has become even more important when the District had to implement a remote learning environment due to the pandemic, requiring all students and staff to have a device that can connect to the District.

**Issue #1:** While the District does have policies on how IT devices should be utilized to safeguard technology resources (i.e., access security protocols), the District does not have formal documented procedures on how to input and track such devices. Furthermore, through interviews and our sampling testing, we noted that some staff were not formally trained on the procedures for inputting the IT inventory records, which resulted in duplicate asset information being entered, as well as missing or inaccurate pieces of key asset information. Specifically, we noted:

- 8 devices did not have the location assigned.
- 21 devices (18 laptops, 1 tablet, and 2 webcams) did not have a user assigned.
- 6 devices (5 laptops and 1 webcam) did not contain the manufacturer.
- 3 devices (2 laptops and 1 tablet) did not contain the serial number.

**Risk:** There is an increased risk of loss or misappropriation of assets which may not be readily detected.

**Level:** Moderate-High

**Recommendation:** We recommend the District create formal written procedures related to the tracking of inventory and ensure all staff involved in inventory management be knowledgeable of the procedures. Furthermore, we recommend that District staff who are responsible for inputting and updating IT inventory records are formally trained.

**Management’s Response and Planned Completion Date:**

*The District has purchased over 8,000 devices during the past fifteen months. Due to the increase of devices that are mobile (student/teacher laptops), the District will update inventory methods to prevent loss and misappropriation of assets. The District is currently working on formal procedures for entering, managing, and reconciling inventory. We expect the updated procedures, along with the training of our Computer Aides and Network & Systems Technician, to be completed by the end*

of the 2021-2022 fiscal year. Training will be conducted by the Administrator of Technology initially; but the Network & Systems Technician will be responsible for future trainings as well as enforcing the updated procedures.

## **II. IT INVENTORY & ASSET MANAGEMENT**

School districts should maintain detailed, up-to-date, complete inventory records for all computer equipment located throughout all buildings. The information maintained for each piece of computer equipment should include the following: an asset tag number and asset description, a serial number, a model number, the user assigned, the date and cost of purchase, the related purchase order number, expected useful life, repair information, and the asset's location (i.e., the specific room and building to which the asset has been assigned). The District can then determine then the life cycle of such assets which facilitates in budgeting for future purchases.

District purchases of IT-related items are generally made through the technology department. The purchasing department flags the purchase orders and files the claims packets separately with a copy of the asset tag. The duplicate copy of the asset tag is then sent to the technology department to tag the devices. Items are then entered into the District's inventory software, FreshWorks, by an employee or by FreshWorks' Discovery Agent ("Agent") after the Agent has been installed on the machine. The Agent collects the machine's hardware and software information and automatically updates the inventory information in FreshWorks. The Agent makes the discovery of assets more efficient, as the device information does not have to be manually entered.

To assess the adequacy and accuracy of the inventory records, we generated a report of all assets from FreshWorks and selected sixty (60) items from the District's inventory listing of those devices that were purchased as a result of the pandemic as follows:

<b>Device Type</b>	<b>Total Devices</b>	<b>Selected for Testing</b>
Hotspot	114	1
Hovercam	31	1
Laptop	7904	50
Tablet	154	2
Temperature Scanners	50	1
Webcam	613	5
<b>Total</b>	<b>8,866</b>	<b>60</b>

For those devices that were assigned to students or staff, we verified whether the District had a completed agreement on file which outlines the assignee's responsibility for the device, signed by the employee, or the student and parent. For the hotspot selected, we reviewed the usage log to verify whether the device was being used by the student. For all other devices, we verified whether the device was at the location as stated in the inventory system and verified whether the inventory records for that device (e.g., tag number, serial number, location, user, etc.) were accurate. In addition, we selected twenty (20) items found at various school buildings throughout the District to verify whether the inventory records captured the asset's data and that the data captured is accurate.

**Issue #2:** We noted the following results from our testing:

**FreshWorks List to Location Test:**

- There were 4 devices (i.e., 3 laptops and 1 hovercam) that could not be located at the time of our audit. Furthermore, the District did not have a completed agreement on file for one of the laptops, and one of the laptops that was assigned to a student had a contract on file but was being used by a sibling. We were informed that the hovercam was in use at the time of our audit but the District was unable to provide proof from the assigned user that the item was still in possession. We were informed that the District is contacting three of the assignees to ensure there is documentation of their possession of the devices.
- There was 1 device (iPad) that was missing the serial number in FreshWorks. However, we were able to locate the item based on its tag number.
- There were 5 devices (all laptops) where the serial number and asset tag per the inventory records does not agree with actual tag and serial number. We were informed this was an incorrect entry in FreshWorks and that there is no device that corresponds with the entry. We discussed the issue with the Technology Director and were informed that the District is working to remove these entries as they are discovered.

**Location to Inventory Within FreshWorks Test:**

- The asset tag for 1 laptop did not agree with tag information listed in FreshWorks. We were able to confirm the device in FreshWorks using the serial number.
- There were 4 devices (all laptops) that did not have the correct device location in FreshWorks.
- 5 of the devices (3 webcams and 2 laptops) selected at the buildings did not have any location indicated in FreshWorks.
- FreshWorks did not have the correct serial number for 1 device (laptop) selected on site. We were able to confirm the existence of the device in FreshWorks using the asset tag number.
- FreshWorks did not contain the serial number for 1 device (laptop) selected on site. We were able to confirm the existence of the device in FreshWorks using the asset tag number.

**Risk:** The District may not be able to adequately safeguard and account for all IT assets, which may lead to unnecessary purchases, inaccurate budgeting, and loss of assets.

**Level:** Moderate-High

**Recommendation:** As noted in issue #1, we recommend the District develop formal written procedures for utilizing the software FreshWorks for tracking inventory. Specifically, the procedures should address how inventory information is added to and updated in FreshWorks. Periodic physical inventory assessments should be performed to ensure the inventory records are complete and accurate. Lastly, users should be restricted from moving devices from their assigned location.

**Management's Response and Planned Completion Date:**

*The District has hired and upgraded personnel to assist with the management of the increased number of technology items. In July and August 2021, eleven part-time Computer Aide positions were converted to full time employees and the District hired a new Network & Systems Technician. The Computer Aides are directly responsible for managing the inventory of technology items within their assigned building. The newly hired Network & Systems Technician will assist in the management and deployment of student 1:1 devices along with managing the District-wide inventory in collaboration with building level Computer Aides. Updated procedures are being developed and will be shared with all Technology Department employees. The Business Office Reference Guide includes information that reiterates the importance of the technology inventory and the movement of any associated devices. Specifically, any such movement cannot happen without first discussing them with the Administrator of Technology. During the 2021-2022 school year, a complete inventory reconciliation will take place to verify what is stored in our asset management system. This should be completed by June 30,2022.*

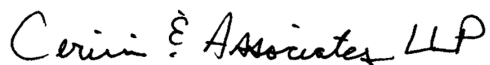
---

We would like to thank the staff at the District for its cooperation and professionalism during our testing.

We understand the fiduciary duty of the Board of Education, as well as the role of the internal auditor in ensuring that the proper control systems are in place and functioning consistently with the Board's policies and procedures.

Should you have any questions regarding anything included in our report, please do not hesitate to contact us at (631) 582-1600.

Sincerely,



Cerini & Associates, LLP  
Internal Auditors